

**IN THE UNITED STATES DISTRICT COURT  
FOR THE SOUTHERN DISTRICT OF ALABAMA  
SOUTHERN DIVISION**

**IN THE MATTER OF THE SEARCH OF  
THE FOLLOWING THREE ELECTRONIC  
DEVICES:**

- 1. EVIDENCE ITEM 1B2: ONE (1)  
SILVER MACBOOK PRO LAPTOP;**
- 2. EVIDENCE ITEM 1B3: ONE (1)  
SAMSUNG DUOS S/N:**

- 3. EVIDENCE ITEM 1B4: ONE (1)  
SAMSUNG DUO GALAXY J1  
PHONE;**

**RECOVERED AT**

**LOCATED AT FBI MOBILE FIELD  
OFFICE  
36602**

Case No.

*23-mj-115-B*

**Filed Under Seal**

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION UNDER RULE 41 FOR A SEARCH WARRANT**

I, Evan Fischer, Special Agent of the Federal Bureau of Investigation (FBI), Mobile Division, being duly sworn and deposed, state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property-electronic devices-which are currently in law enforcement possession, and extraction from that property of electronically stored information described in Attachment B.

2. I have been a law enforcement officer for approximately twelve years. I am currently employed with the Federal Bureau of Investigation ("FBI") as a Special Agent and have been since July 31, 2022. I am currently assigned to the Violent Crime Major Offenders squad. I

investigate domestic violent incident crimes, which include criminal organization narcotics investigations, bank robberies, commercial / armored car robberies, fugitives, kidnappings, threats and / or assaults of federal officials, police killings, and mass killings. I have also received training on obtaining and reviewing electronic records, including telephonic and e-mail communications. As part of my investigations, I routinely collect and review electronic evidence, including data gathered from social media accounts. Prior to the FBI, I was employed as an Officer with the Austin Police Department (PD) in Austin, Texas for approximately six years and prior to Austin PD, I was employed as an Officer with United States Customs and Border Protection for approximately five years. As such, I am an investigative or law enforcement officer of the United States within the meaning of Title 18, United States Code 2510(7), that is, an officer of the United States who is empowered by law to conduct investigations of and to make arrests for offenses enumerated in Title 18, United States Code, Section 2516(1). I have also received training on obtaining and reviewing electronic records, including telephonic and e-mail communications. As part of my investigations, I routinely collect and review electronic evidence, including data gathered from social media accounts.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

**IDENTIFICATION OF THE DEVICE TO BE EXAMINED**

4. The property to be searched is a SILVER MACBOOK PRO LAPTOP, a SAMSUNG DUOS S/N: 1 3; and a SAMSUNG DUO GALAXY J1 PHONE , hereinafter the "Devices." The Devices are currently located at FBI Mobile Field Office, located

at 200 N. Royal St. Mobile, AL 36602.

5. The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

6. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 875(c) (Threatening Interstate Communications); 18 U.S.C. § 1952 (Interstate and foreign travel or transportation in aid of racketeering enterprises); 18 U.S.C. § 2421 (Transportation); 18 U.S.C. § 2421A (Promotion or Facilitation of Prostitution and Reckless Disregard of Sex Trafficking) and 8 U.S.C. § 1328 (Importation of alien for immoral purpose)

in the Southern District of Alabama and elsewhere and that evidence of these violations will be found on the items to be searched, described in attachment A.

**PROBABLE CAUSE**



*Image 1. Screenshot of message sent to Victim-1.*



























**TECHNICAL TERMS**

31. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.
- b. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to

another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.

- c. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 “wi-fi” networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.
- d. IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be

assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

- e. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- f. Google Voice is an application that “gives you a phone number for calling, text messaging, and voicemail. It works on smartphones and computers, and syncs across your devices so you can use the app in the office, at home, or on the go.”<sup>1</sup>

32. Based on my training, experience, and research I know that the Devices have capabilities that allow them to serve as “a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA.” In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

**ELECTRONIC STORAGE AND FORENSIC ANALYSIS**

33. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

34. There is probable cause to believe that things that were once stored on the Device may still be stored there, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

35. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store

configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

36. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

37. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

### **CONCLUSION**

38. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

### **REQUEST FOR SEALING**

39. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the warrant is relevant



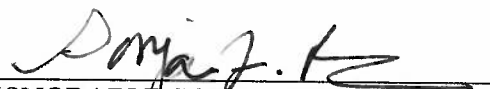
to an ongoing investigation into the criminal organizations as not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that, online criminals actively search for criminal affidavits and search warrants via the internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,



EVAN FISCHER  
Special Agent  
Federal Bureau of Investigation

THE ABOVE AGENT HAD ATTESTED  
TO THIS AFFIDAVIT PURSUANT TO  
FED. R. CRIM. P. 4.1(b)(2)(A) THIS  
5th, MAY \_\_\_\_\_, 2023.

  
HONORABLE SONJA BIVINS  
UNITED STATES MAGISTRATE JUDGE

Certified to be a true and  
correct copy of the original.  
Charles R. Diard, Jr.  
U.S. District Court  
Southern District of Alabama

By: Shannon Davison  
Deputy Clerk

Date: May 05, 2023



**ATTACHMENT A**

**PROPERTY TO BE SEARCHED**

The property to be searched is the following: EVIDENCE ITEM 1B2: ONE (1) SILVER MACBOOK PRO LAPTOP; EVIDENCE ITEM 1B3: ONE (1) SAMSUNG DUOS S/N: ; EVIDENCE ITEM 1B4: ONE (1) SAMSUNG DUO GALAXY J1 PHONE; and the SIM CARDS RECOVERED WITH THE ABOVE-LISTED SAMSUNG PHONES which were recovered at [REDACTED] pursuant to a federal search warrant, and currently located at FBI Mobile Field Office 200 N.Royal St Mobile, AL 36602.

This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

**ATTACHMENT B**

**Particular Things to be Seized**

All records and electronic data relating to violations of 18 U.S.C. § 875(c); 18 U.S.C. § 1952; 18 U.S.C. § 2421; 18 U.S.C. § 2421A, and 8 U.S.C. § 1328 involving other known and unknown individuals, including:

- a. Any records on the Devices described in Attachment A that relate to violations of the specified federal offenses including:
  - a. Records, documents, programs, applications, or material related to the specified federal offenses;
  - b. Any stored or deleted SMS and MMS messages, iMessages, email messages, voicemails, call history, address books, multimedia messages, browser history, or location history relating to the specified federal offenses;
  - c. Any stored or deleted information from messaging applications, social media applications, or email applications relating to the specified federal offenses;
  - d. Any stored or deleted photographs, in any location, related to the specified federal offenses;
  - e. Records of Internet activity, including firewall logs, caches, browser history and cookies, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

- f. Any stored or deleted audio recordings, photographs, video recordings, still images, or screen captures sent to or taken by ----- related to the specified federal offenses;
- g. Information regarding the acquisition and use of applications, phone number(s), including payment method, subscriber records, periods of use, call records, text message records, including content, and other information which might further identify the user of the phone numbers utilized by the devices listed in Attachment A;
- h. Evidence indicating how and when accounts were accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the specified federal offenses and to the account owner;
- i. The identity of the person(s) who created or used the account, including records that help reveal the whereabouts of such person(s);
- j. Any available location data relating to the specified federal offenses;
- k. Any information regarding the deletion of data related to the specified federal offenses, including, but not limited to, the clearing of location history, browser history, or other files;
- l. Any and all visual depictions of individuals engaged in, or suggesting, sexually explicit conduct, as defined in 18 U.S.C. § 2256;
- m. Any evidence of monetary transactions, communications pertaining to financial records, division of proceeds, recordings, the pickup or sale of items, and meeting locations as well as times of meetings related to the specified federal offenses;

- n. Lists of commercial sex customers and related identifying information related to the specified federal offenses;
  - o. Types, amounts, and prices of commercial sex transactions, as well as dates, places, and amounts of specific transactions related to the specified federal offenses;
  - p. All bank records, checks, credit card bills, account information, records relating to cryptocurrency, and other financial records related to the specified federal offenses;
  - q. Any information recording [redacted]'s schedule or travel from approximately January 01, 2017 to the present related to the specified federal offenses;
  - r. Evidence of the attachment of other devices or use of applications used to transfer data off of the Devices; and
  - s. Evidence of the presence or absence of software that would allow others to control the Devices, such as viruses or other malware, as well as evidence of the presence or absence of security software designed to detect malware.
- b. Evidence of user attribution showing who used, owned, paid for, controlled, or accessed the Devices (and/or accounts on the Devices) at the time the things described in this warrant were created, edited, or deleted, including, but not limited to, logs, phonebooks, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs; any form of text messages, including the content of the text messages, videos, photographs, and correspondence, including information to assist in locating the whereabouts of such person(s);
- c. Records evidencing the use of the Internet including:

- a. records of Internet Protocol addresses used;
- b. records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.